UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/402,144	09/29/1999	MARTINA HANCK	P991784	5593

29177 7590 01/11/2006

BELL, BOYD & LLOYD, LLC
P. O. BOX 1135
CHICAGO, IL 60690-1135

EXAMINER	
KIM, JUNG W	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 01/11/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/402,144	HANCK ET AL.	
	Examiner	Art Unit	
	Jung W. Kim	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 December 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3,10-12,19-34 and 36-48* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,10-12,19-34 and 36-48* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This Office action is in response to the RCE filed on December 2, 2005.

2. Claims 1-3, 10-12, 19-34 and 36-48 are pending.

3. Claims 1-3, 10-12 and 36 are amended.

4. Claim 4-9, 13-18 and 35 are canceled.

5. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Continued Examination Under 37 CFR 1.114

6. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on December 2, 2005 has been entered.

Response to Arguments

7. In reply to Applicant's argument that the Halsall reference does not teach the new limitation wherein the data segments are grouped irrespective of their original order since the cyclic redundancy method requires a specific order before they are grouped (pg. 10, 4th and 5th paragraph), the block sum check method taught by Halsall covers

the new limitation since a specific order is not required. Moreover, the new limitation of the first and second segment checksum values being hashes have been found to be obvious enhancements as outlined below. Hence, the instant claims remain rejected under the prior art of record.

Claim Rejections - 35 USC § 112

8. Claim 36 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

9. Claim 36 recites the limitation "said first segment checksum" in line 2. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 103

10. Claims 1-3, 10, 22-33, 37, 40, 43 and 46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Halsall, Data Communications, Computer Networks and Open Systems 4th Edition (hereinafter Halsall) in view of Frezza et al. U.S. Patent No. 4,982,430 (hereinafter Frezza).

11. As per claim 10, Halsall teaches a block sum check, also known as a two-dimensional parity check, which forms a commutative checksum on digital data. This block sum check is arranged as follows:

a. digital data is grouped into several data segments irrespective of each data segment's original order by a computer and processed to form a first segment checksum for each data segment. The first segment checksum constitutes the assignment of an odd or even parity bit to each block. This assignment is given the operational name of row parity (Halsall, page 129, 1st paragraph);

b. the first segment checksums are processed to form a first commutative checksum (Halsall, page 129, 1st paragraph). The first commutative checksum constitutes an assignment of a parity bit (odd or even) for each bit position for all the blocks of a message, including the parity bit position of each block. This assignment is given the operational name of column parity and the block comprising the column parity bits is the first commutative checksum. In addition, Halsall teaches using an XOR operation to establish parity, which is a commutative operation (Halsall, page 128, Figure 3.14);

c. the arrangement is incorporated into the sending side of a pair of Data Terminal Equipment (DTE) (see Halsall, page 125, section 3.4 and page 128, section 3.4.2). Conventionally, DTE incorporates at least one arithmetic/logic unit: ALUs are the basic units required in hardware to perform arithmetic and logic microoperations.

12. Although Halsall does not cover a cryptographic operation to protect the first commutative checksum in this section (the section covers error detection methods), Halsall in a different section teaches data encryption operations as standard

implementations on transmissions that require privacy on an unprotected network (Halsall, page 719, 2nd paragraph). However, Halsall does not expressly teach cryptographically protecting integrity values of a message. Frezza teaches encrypting integrity values to prevent unauthorized alteration of a message. Frezza, col. 2:45-3:13. It would be obvious to one of ordinary skill in the art at the time the invention was made to implement a cryptographic operation to secure the first commutative checksum. One would be motivated to do so to prevent an unscrupulous third party from an unauthorized modification of a transmitted message (Frezza, col. 2:20-25). The aforementioned cover claim 10.

13. As per claim 37, Halsall in view of Frezza cover the following: 1) an arrangement for forming a first commutative checksum, 2) an arrangement for checking a predetermined cryptographic commutative checksum, and 3) an arrangement for forming and checking a first commutative checksum as outlined above in the claim 10 rejection 35 U.S.C. 103(a). In addition, the cryptographic operations described use a symmetric key methodology (Halsall, page 723, 1st paragraph).

14. As per claims 40, Halsall in view of Frezza cover the following: 1) an arrangement for forming a first commutative checksum, 2) an arrangement for checking a predetermined cryptographic commutative checksum, and 3) an arrangement for forming and checking a first commutative checksum as outlined above in the claim 10 rejection under 35 U.S.C. 103(a). In addition, Halsall teaches the commutative

operation to establish column parity, which forms the commutative checksums, is an XOR operation (Halsall, page 127, section 3.4.1): the XOR operation exhibits both commutative and associative properties. Furthermore, control of the data inputs to the arithmetic circuits of the ALU determines the type of operation executed by the ALU. The aforementioned cover the limitation of claim 40.

15. As per claim 43, Halsall in view of Frezza cover an arrangement as outlined above in the claim 10 rejection under 35 U.S.C. 103(a). Halsall does not expressly disclose archiving the digital data and the cryptographic commutative checksum. However, archiving the elements of a transmission is a standard feature to verify the contents of a transmission to an auditor. The examiner takes Official Notice that archiving transmission elements are standard means to record the transmission to prove the contents and status of the transmission at a latter date (i.e. auditing a transmission). It would be obvious to one of ordinary skill in the art at the time the invention was made to archive the digital data and the checksum since it preserves a receipt of the transmission. The aforementioned cover the limitations of claim 43.

16. As per claim 46, Halsall in view of Frezza cover the following: 1) an arrangement for forming a first commutative checksum, 2) an arrangement for checking a predetermined cryptographic commutative checksum, and 3) an arrangement for forming and checking a first commutative checksum as outlined above in the claim 10 rejections under 35 U.S.C. 103(a). In addition, as mentioned previously, the digital data

is cryptographically protected, and by convention, the cryptographic operation would be implemented by an ALU. Furthermore, since Halsall teaches the arrangements in the context of a digital network, the digital data would necessarily be processed in accordance with a network management protocol. The aforementioned cover the limitation of claim 46.

17. As per claims 1-3 and 22-33, they are method claims corresponding to the subject matter covered in the rejections of claims 10, 37, 40, 43 and 46, and they do not teach or define above the information covered in the rejections of claims 10, 37, 40, 43 and 46. Therefore, claims 1-3 and 22-33 are rejected under Halsall in view of Frezza for the same reasons set forth in the rejections of claims 10, 37, 40, 43 and 46.

18. Claims 11, 12, 19-21, 34, 36, 38, 39, 41, 42, 44, 45, 47 and 48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Halsall in view of Frezza, and further in view of Mattison USPN 5,778,070 (hereinafter Mattison).

19. As per claim 11, Halsall in view of Frezza cover an arrangement as outlined above in the claim 10 rejection under 35 U.S.C. 103(a). In addition, the arrangement also includes the following:

d. the allocation of the predetermined cryptographic checksum to the digital data and the subjection of the cryptographic commutative checksum to an inverse cryptographic operation to form a first commutative checksum (Halsall,

page 723, 1st paragraph). Halsall teaches any message encrypted by DES has an inverse operation (decryption) to retrieve the original message (Halsall, page 723, 1st paragraph). Furthermore, every ciphertext is associated with a specific plaintext;

e. the formation of a second segment checksum for each data segment, the formation of a second commutative checksum by a commutative operation on the second segment checksums, and a comparison of the first commutative checksum and the second commutative checksum for a match (Halsall, page 129, Figure 3.15 (b)).

20. Halsall does not teach the second segment checksum is formed in accordance with a type selected from the group consisting of a hashing value and a cryptographic one-way function. However, the use of a hashing value as a checksum is a well known means to ensure the integrity of a data segment. For example, Mattison discloses hashing as a more rigorous means than a typical checksum to ensure data integrity since a hash of a data block is unique to that data block and any modification to the data block will modify the hash (5:20-34). Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the segment checksum to be a hashing value. One would be motivated to do so to establish a more rigorous integrity check on the data segments. The aforementioned cover the limitations of claim 11.

21. As per claim 12, since the second segment checksum (the checksum to verify an integrity value) is a hash value, the first segment checksum (the checksum to form an integrity value) is also a hash value. Hence, the above arrangements outlined in the claim 10 and 11 rejections under 35 U.S.C. 103(a) together covers the arrangement outlined in claim 12.

22. As per claims 34 and 36, they are method claims corresponding to claims 11 and 12, and they do not teach or define above the information claimed in claims 11 and 12. Therefore, claims 34 and 36 are rejected under Halsall in view of Frezza and Mattison for the same reasons set forth in the rejections of claims 11 and 12.

23. As per claims 38 and 39, Halsall in view of Frezza and Mattison cover the following: 1) an arrangement for forming a first commutative checksum, 2) an arrangement for checking a predetermined cryptographic commutative checksum, and 3) an arrangement for forming and checking a first commutative checksum as outlined above in the claim 11 and 12 rejections under 35 U.S.C. 103(a). In addition, the cryptographic operations described use a symmetric key methodology (Halsall, page 723, 1st paragraph).

24. As per claims 41 and 42, Halsall in view of Frezza and Mattison cover the following: 1) an arrangement for forming a first commutative checksum, 2) an arrangement for checking a predetermined cryptographic commutative checksum, and

3) an arrangement for forming and checking a first commutative checksum as outlined above in the claim 11 and 12 rejections under 35 U.S.C. 103(a). In addition, Halsall teaches the commutative operation to establish column parity, which forms the commutative checksums, is an XOR operation (Halsall, page 127, section 3.4.1): the XOR operation exhibits both commutative and associative properties. Furthermore, control of the data inputs to the arithmetic circuits of the ALU determines the type of operation executed by the ALU. The aforementioned cover the limitations of claims 41 and 42.

25. As per claims 44 and 45, Halsall in view of Frezza and Mattison cover an arrangement as outlined above in the claim 11 and 12 rejections under 35 U.S.C. 103(a). Halsall does not expressly disclose archiving the digital data and the cryptographic commutative checksum. However, archiving the elements of a transmission is a standard feature to verify the contents of a transmission to an auditor. The examiner takes Official Notice that archiving transmission elements are standard means to record the transmission to prove the contents and status of the transmission at a latter date (i.e. auditing a transmission). It would be obvious to one of ordinary skill in the art at the time the invention was made to archive the digital data and the checksum since it preserves a receipt of the transmission. The aforementioned cover the limitations of claims 44 and 45.

26. As per claims 47 and 48, Halsall in view of Frezza and Mattison cover the following: 1) an arrangement for forming a first commutative checksum, 2) an arrangement for checking a predetermined cryptographic commutative checksum, and 3) an arrangement for forming and checking a first commutative checksum as outlined above in the claim 11 and 12 rejections under 35 U.S.C. 103(a). In addition, as mentioned previously, the digital data is cryptographically protected, and by convention, the cryptographic operation would be implemented by an ALU. Furthermore, since Halsall teaches the arrangements in the context of a digital network, the digital data would necessarily be processed in accordance with a network management protocol. The aforementioned cover the limitations of claims 47 and 48.

27. As per claims 19-21, they are method claims corresponding to claims 11, 12, 34 and 36 and they do not teach or define above the information claimed in claims 11, 12, 34 and 36. Therefore, claims 19-21 are rejected under Halsall in view of Frezza and Mattison for the same reasons set forth in the rejections of claims 11, 12, 34 and 36.

Communications Inquiry

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W. Kim whose telephone number is 571-272-3804. The examiner can normally be reached on M-F 9:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jung W Kim
Examiner
Art Unit 2132

January 5, 2006

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100